DHS Science and Technology Directorate

Homeland Open Source Technology

Doing more with less and more securely

Cybersecurity threats are continuously adapting to new defenses, requiring government and the broader community to constantly pursue innovative new approaches. In order for governments at the federal, state and local level to successfully accomplish this, they have to engage the broader market; examine all potential solutions; and have processes in place to quickly acquire and deploy new technologies. This can be challenging due to the specialized government certification and procurement requirements, which in turn limit the pool of available solutions. Limited funding dedicated to information technology and security will only make it more difficult to keep abreast with continually advancing cyber threats.

Leveraging a broader marketplace

Open source software (OSS) provides many innovative security solutions that government is not yet successfully leveraging. OSS is software where the source code is available for use, modification and redistribution. Active OSS projects produce rapid innovations and encourage inclusive development, making them more responsive to specialized requirements. If something needs to be modified, you can access the code and make the change. This flexibility, coupled with the rapid pace of innovation, makes open source security technology an important solution source, which is important for the government to leverage.

Homeland Open Source Technology (HOST) is working to enable better use of OSS by the government. Some of the major obstacles preventing the widespread government adoption of OSS include a lack of an acknowledged governance structure, qualified and trusted information, and documentation, reliable resource availability, standardized information assurance, security vetting processes and open communication with independent open technology development and support communities.

Open Source Discovery Efforts

The HOST program is investigating new and existing open security projects and techniques that support and protect government cyber assets. This is being achieved through the development and sharing of comprehensive public accessible inventory of open source projects, tools and applications, as well as best practices and lessons learned.

Open Source Collaboration Efforts

Coordinating development activities and encouraging working relationships between public and private-sector research and development communities, is critical to increasing the sustainable use of Open Security Technology. Cross-industry events designed to serve as platforms for collaboration are currently underway.

Open Source Investment Efforts

The Department of Homeland Security **(**DHS), Science and Technology Directorate is committed to providing seed investments in advanced research and development activities that support national cybersecurity objectives and have the potential to create sustainable project communities. This is achieved in part by enabling broad adoption and participation by public and private-sectors.

Initial sponsorships are focused on developing the first open source, multi-threaded intrusion detection system, called *Suricata*, and validating the latest version of Open Secure Socket Layer, a common encryption library, against the Federal Information Processing Standard 140-2 (FIPS 140-2). Now fully developed, validated and transitioned, these seed investments are examples of cybersecurity innovations that, through open source licensing, provide lower cost solutions for use by federal, state and local government agencies.

Homeland Security
Science and Technology

To learn more about Homeland Open Security Technology, contact sandt-cyber-liaison@hq.dhs.gov.

2014-11-03